REMARKS

Claims 21-31 are pending. Claims 21-31 stand rejected. Claim 21 has been amended to correct a typographical error. As such, Applicants request that the amendment be admitted, even though the office action was a final office action. Further, applicants respectfully submit that the Office Action was improperly made final because the Office Action uses a new grounds of rejection. As such, applicants respectfully submit the amendments presented herein should be admitted as of right. If the Office Action is found to have properly been made final, however, applicants nevertheless respectfully submit that the amendments proposed should be admitted since the amendments correct minor errors and/or raise no new issues with regard to patentability, and would place the application in better form for appeal. Applicants respectfully request reconsideration of the rejections in light of the arguments presented.

35 U.S.C. § 103 Rejections

Status

Claims 21-31 stand rejected under 35 U.S.C. § 103 as being anticipated by Stenberg (International Publication No. WO 011/3666) in view of Rezaiifar et al. (U.S Patent Publication No. 2003/0055964).

Cited Reference - Stenberg

Stenberg describes a method for authenticating a mobile terminal in a hybrid network architecture (e.g., DTETRA network), resulting from the combination of a TETRA network (radio access network layer) and a GSM network (overlaying network layer).

According to the method proposed in Stenberg, for compatibility reasons in the respective authentication procedures performed in GSM and TETRA networks, the authentication parameters of the TETRA radio access network layer are derived from the GSM authentication parameters. Conversely, the mobile terminal is adapted to restore GSM authentication parameters from TETRA authentication parameters.

The authentication method proposed in Stenberg aims at enabling the authentication of a user in a hybrid network architecture composed of ***two layers***, which rely respectively on two distinct and independent networks (the TETRA and the GSM networks). Those networks have two distinct authentication mechanisms, which are incompatible with each other, as they do not use the same type of authentication data (see Stenberg page 8 lines 8-9 and lines 26-29). The authentication method proposed in Stenberg enables the two authentication procedures performed respectively on TETRA network and GSM network to interact with each other, to enable a terminal to connect to the hybrid DTETRA network and benefit from the services offered by this network (e.g. roaming between GSM and TETRA, etc.).

Cited Reference - Rezaiifar

Rezaiifar describes a method and an apparatus for authorizing an access terminal requesting a service provided by an entity in an access network (abstract). More particularly, each service is authorized by a distinct Service Selector ("SS"), which verifies that the terminal requesting the service is authorized to use the service. If this is the case, the SS selects a service provider to provide the service to the user, in accordance with the user terminal's capabilities ([0036]). To do so, an authentication of the terminal is carried out by an AAA server (RADIUS) to authorize a session of communication ([0036]). This authentication is based in one particular embodiment on CHAP protocol ([0038]). Once the terminal is authorized to use the communication link, it receives an ***IP address*** of the SS and can send a service query to this SS ([0040]).

This service query comprises a ***source address*** (the IP address of the terminal), a ***destination address*** (the IP address of the SS) and the terminal's capabilities to determine the service to be provided ([0040]). A BSC/PCF receives the service query, and if it determines that the terminal is attempting to contact the SS for the first time, it sends the SS a message comprising the IP address of the terminal and the RADIUS attributes of the terminal obtained during the authorization procedure carried out by the AAA server ([0042]). The SS then performs service authorization in accordance with the RADIUS attributes ([0042]), and if the service is authorized, selects a service provider in accordance to the terminal's capabilities.

Independent claims

The independent claims include features neither disclosed nor suggested by the cited references, either alone or in combination, namely as represented by claim 21:

> 21. (Currently Amended) A method for authenticating a user for access to at least two entities of a data transmission network by means of a terminal, which method includes the following series of steps:
>
> - a random number is transmitted to the terminal,
> - data for ***authenticating the user to the two entities of the network*** is calculated using at least one predefined cryptographic algorithm applied to the random number received and at least one secret key specific to the user,
> - the terminal inserts, in an access request, data for identifying the user to said two entities of the network and the calculated authentication data, and transmits the access request to an access controller, wherein ***the inserted data for authenticating the user comprises a distinct set of data for each of the two entities***;
> - ***the access controller transmits, to each of the two entities***, a respective authentication request containing the identification data and the distinct set of inserted data for authenticating the user to the respective entity of the network, contained in the access request,
> - authentication servers of the entities carry out a user authentication procedure, on the basis of user identification and authentication data, contained in the authentication requests, and
> - authentication reports containing results of the authentication procedures carried out by the authentication servers of each of said two network entities are transmitted to the terminal. (emphasis added)

The cited sections of Stenberg do not disclose or suggest "authenticating the user to the ***two entities*** of the network," as recited by claim 21. The cited section [claim 5], discloses one or more session authentication key, but nowhere indicates that the multiple session keys are used for ***two entities*** of a network. In contrast, Stenberg is clear that it is directed to enabling authentication of a user in a ***hybrid*** network architecture composed of ***two layers***, which rely respectively on two distinct and independent networks, that is the TETRA and the GSM networks. As such, Stenberg also does not disclose or suggest that an "access controller transmits, to each of the ***two entities***, a respective authentication request," as recited by claim 21.

The problem being solved in Stenberg is quite different from the problem faced by the instant inventors who did not aim at making consistent two authentication procedures performed on two ***different networks***, but aim at simplifying, for example, the authentication of a terminal to ***two distinct and independent entities*** of a network (e.g., two service providers), to which the terminal can access independently one from the other. Those two entities can have separate and independent authentication procedures (which can be conducted in parallel to access simultaneously the two entities). Thus, when a terminal connects to the network and wants to access both entities, authentication of the terminal to those entities is simplified. Moreover, because the entities can be independent and distinct, simultaneous authentication could be possible. Stenberg does not authorize performing in parallel both authentications due to the hybrid nature of the DTETRA network. Further, sending a unique access request comprising identification and authentication data to both the GSM network and to the TETRA network does not makes sense in the context of roaming as described in Stenberg.

Stenberg also fails to disclose or suggest that "the ***inserted data*** for ***authenticating*** the user comprises a ***distinct set of data for each of the two entities***," as recited by the claims. This makes sense because Stenberg does not discuss authentication to two entities and thus would not need to consider distinct sets of data for the two entities. The examiner notes this deficiency in Stenberg, and relies on Rezaiifar for such disclosure.

Rezaiifar, however, does not cure the deficiencies of Stenberg. Rezaiifar does not describe inserted data for authenticating the user that includes a distinct set of data for each of the two entities. The cited section of Rezaiifar [paragraph 0040] only describes the insertion of an IP address of the terminal and an IP address of the service selector. Those IP addresses provide neither data for authenticating the user (nor data for identifying the user) to two entities of a network, as recited in claim 21. At most, these IP addresses ***identify the user's terminal*** and the service selector, but does not provide authentication information for two entities of a network. (Similarly, the terminal's compatibility data inserted by itself in the service query are not identification data nor authentication data to two entities of a network.)

Further, Rezaiifar does not describe an ***access controller*** which transmits to each of the ***two entities***, a respective authentication request containing the identification data and the authentication data to the respective entity of the network contained in the access request.

Claims 25, 27, and 29 include similar features to those described above in connection with claim 21 and are patentable for similar reasons. Claims 22-24, 26, 28, and 30-31 each depend from one of independent claims 21, 25, 27, or 29, and are therefore allowable for at least the reasons given above. Applicants therefore respectfully request that the Examiner withdraw the rejections of claims 21-31.

CONCLUSION

For all the foregoing reasons, Applicants respectfully submit that the application is in condition for allowance.

Please charge any required fees and apply any other charges or credits to deposit account 06-1050 referencing attorney docket no. 18394-0017US1.

Respectfully submitted,

Date: May 7, 2009

Raymond N. Scott, Jr.
Reg. No. 48,666

Fish & Richardson P.C.
P.O. Box 1022
Minneapolis, MN 55440-1022
Telephone: (302) 652-5070
Facsimile: (877) 769-7945